IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Steven Tischer	)
		) Group Art Unit:
Serial No.:	10/735,931	) 2416
		) Examiner:
Filed:	December 15, 2003	) Haile
		)
For:	SYSTEMS, METHODS, AND STORAGE MEDIUM FOR TRANSMITTING DATA OVER A COMPUTER NETWORK	)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

REAL PARTY IN INTEREST

The real party in interest is AT&T Intellectual Property I, L.P., an entity owning certain assets of BellSouth Intellectual Property Corporation, the assignee of record.

RELATED APPEALS AND INTERFERENCES

There are no pending appeals or interferences related to this appeal.

STATUS OF CLAIMS

Claims 5 and 16 have been canceled.

Claims 1-4, 6-15 and 17-21 stand finally rejected.

The rejections of claims 1-4, 6-15 and 17-21 are herein appealed.

STATUS OF AMENDMENTS

There have been no amendments filed after the final rejection mailed October 17, 2008.

SUMMARY OF CLAIMED SUBJECT MATTER

A concise explanation of the subject matter defined in each of the independent claims involved in the appeal is provided below.

Independent claim 1 recites a method for transmitting data over a computer network to a predetermined recipient, the method comprising: modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message (paragraph [0037]; Figure 11A, element 236), the first message modification key value being determined based on at least one variable parameter (paragraphs [0023]-[0024]); modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (paragraph [0043]; Figure 11B, element 248), the second message modification key value being determined based on at least one variable parameter (paragraphs [0026]-[0027]); transmitting the first and second modified data messages to a first device (Figure 11A, element 238; Figure 11B, element 250); determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value (paragraphs [0048]-[0050]; Figure 11C, elements 258-262); and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value (paragraphs [0052]-[0054]; Figure 11C, elements 266-270), wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (paragraph [0022]); wherein the first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient (paragraphs [0023] and [0024]), the unique identifier being a biometric identifier obtained from the recipient (paragraph [0024]).

Independent claim 11 recites a system for transmitting data over a computer network to a predetermined recipient, the system comprising: a first device (Figure 1, element 12) configured to modify at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message (paragraph [0037]; Figure 11A, element 236), the first message modification key value being determined based on at least one variable parameter (paragraphs [0023]-[0024]), the first

device further configured to modify at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (paragraph [0043}; Figure 11B, element 248), the second message modification key value being determined based on at least one variable parameter (paragraphs[0026]-[0027]), the first device configured to transmit the first and second modified data messages (Figure 11A, element 238; Figure 11B, element 250); and a second device (Figure 1, element 14) configured to receive the transmitted first and second modified data messages and to determine the first data message for the predetermined recipient based on the modified first data message and the first message modification key value (paragraphs [0048]-[0050]; Figure 11C, elements 258-262), the second device further configured to determine the second data message for the predetermined recipient based on the modified second data message and the second message modification key value (paragraphs [0052]-[0054]; Figure 11C, elements 266-270), wherein the first device is configured to modify multiple bytes of a first data message by adding the first message modification key byte value to multiple bytes of the first data message (paragraphs [0023] and [0024]); wherein the first message modification key value is determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient (paragraph [0024]).

Independent claim 21 recites a computer-readable storage medium encoded with computer-readable computer program code for transmitting data over a computer network, the storage medium including instructions for causing at least one network element to implement a method comprising: modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message (paragraph [0037]; Figure 11A, element 236), the first message modification key value being determined based on at least one variable parameter (paragraphs [0023]-[0024]); modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (paragraph [0043]; Figure 11B, element 248), the second message modification key value being determined based on at least one variable parameter (paragraphs [0026]-[0027]); transmitting the first and second modified data messages to a first device (Figure 11A, element 238; Figure 11B, element 250); determining the first data message in the first

device for the predetermined recipient based on the modified first data message and the first message modification key value (paragraphs [0048]-[0050]; Figure 11C, elements 258-262); and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value (paragraphs [0052]-[0054]; Figure 11C, elements 266-270), wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (paragraph [0022]); wherein the first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient (paragraphs [0023] and [0024]), the unique identifier being a biometric identifier obtained from the recipient (paragraph [0024]).

The above exemplary embodiments are discussed with respect to the aforementioned independent claims by way of example only and are not intended to in any way limit the scope of these claims.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-4, 6, 7, 11-15, 17, 18 and 21 were rejected under 35 U.S.C. § 103 as being unpatentable over Labaton in view of Odagawa.

Claims 8-10, 19 and 20 were rejected under 35 U.S.C. § 103 as being unpatentable over Labaton in view of Odagawa and Kamperman.

ARGUMENT

I. Rejection of claims 1-4, 6, 7, 11-15, 17, 18 and 21

Claims 1-4, 6, 7, 11-15, 17, 18 and 21 were rejected under 35 U.S.C. § 103 as being unpatentable over Labaton in view of Odagawa. This rejection is traversed for the following reasons.

Claim 1 recites, *inter alia,* "modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message . . . wherein the first message modification key value being determined based on the at least one variable parameter and a **unique identifier identifying the**

predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient (emphasis added)." Support for this feature is found in at least paragraph [0024] of Applicant's specification.

Claim 1 relates to transmitted data. A message is modified based on a modification key and the modified data message is transmitted to a first device. One novel and unobvious feature of claim 1 is that the message modification key is determined based on a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient. It is important to keep the context of the "unique identifier identifying the predetermined recipient" in mind when interpreting claim 1. This unique identifier is used in the transmission of a message **to a recipient**. The unique identifier is not used by the recipient at the receiving end, rather, the unique identifier is used in modifying the message prior to transmission. No combination of Labaton and Odagawa teaches or suggests these elements.

Labaton does teach a data transmission system and is related to encrypting messages. Labaton teaches using an "identifier" to modify a message. Column 5, lines 10-19 of Labaton discusses a PIN that is used by the **sender** of a message to encrypt a transmission. However, Labaton fails to teach a unique identifier **identifying the recipient** used in modifying the message. The PIN in Labaton is not related to a predetermined **recipient,** but rather is related to the sender of the message.

As noted by the Examiner, Labaton fails to teach a unique identifier associated with the predetermined recipient used as part of a first message modification key value. The Examiner relies on Odagawa as allegedly teaching "a first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient." Applicant respectfully disagrees with this interpretation of Odagawa.

Odagawa teaches using biometric information from a requester of a product or service as part of a verification process to determine if the requester is entitled access to the product or service. In Odagawa, the biometrics information is not used to determined a message modification key as recited in claim 1. In Odagawa, the biometrics information 44 and variable information 45 are encrypted and sent to an authenticator 12

(See paragraph [0129]). The requester 11 and authenticator 12 use public and private encryption keys as known in the art to transmit the combined biometrics information 44 and variable information 45 in a secure manner. When the authenticator 12 receives the encrypted biometrics information 44 and variable information 45, it decrypts the information and compares the biometrics information 44 and variable information 45 to known values to authenticate the requester (paragraph [0131]). Thus, in Odagawa the biometrics information is not used as a message modification key. The biometrics information in Odagawa is the information being modified by the encryption key. The biometric information is **not** used to determine a first message modification key value as recited in claim 1. Rather, the biometric information in Odagawa is the information that is modified by the encryption key. Thus, the combination of Labaton and Odagawa fails to teach the elements of claim 1.

Further, it is not clear how the Examiner proposes combining Labaton and Odagawa. Labaton relates to a messaging system that encrypts confidential data using a variable (e.g., time). Odagawa teaches encrypting variable information and biometric information to authenticate a user. To arrive at claim 1, one would need to use the biometric information in Odagawa as part of the encryption process in Labaton. This combination is flawed for multiple reasons. First, there is no teaching in Odagawa of using biometric information to encrypt other information. The biometric information is encrypted and used to authenticate a requester.

Second, the sender in Labaton would need to have the recipient's biometric information in order to use it for encrypting a message. This is expressly discouraged in Odagawa. Odagawa repeatedly states that it is desirable to prevent a third party from detecting fixed information that is unique to the authentication requester (e.g., biometrics). For example, in paragraph [0134] Odagawa states "[e]ven if a third party should detect the presented information 14 from a signal during an authentication request, it would therefore be difficult to extract the biometrics information 44 from the presented information 14. Accordingly, this embodiment makes it possible to curtail the risk of a third party posing as the authentication requester 11 and succeeding at authentication." As a primary goal in Odagawa is protecting the biometrics information, Odagawa clearly

teaches against giving the biometrics information to a message sender so the message sender can use the biometrics information to encode a message.

Although The Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in *KSR International Co. v. Teleflex Inc.* relaxed the standards for finding obviousness, the *KSR* decision maintains the doctrine of teaching away. The Court cited the principle that "when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious." In the present case the proposed combination of Labaton and Odagawa is not obvious as the combination is taught against in Odagawa. Further, even if the references are somehow combined, the combination fails to teach the elements of claim 1.

For at least the above reasons, claim 1 is patentable over Labaton in view of Odagawa. Claims 2-4, 6 and 7 variously depend from claim 1 and are patentable over Labaton in view of Odagawa for at least the reasons advanced with reference to claim 1.

Claim 11 recites "wherein the first message modification key value is determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient." As noted above, the combination of Labaton in view of Odagawa fails to teach this feature. Thus, claim 11 is patentable over Labaton in view of Odagawa. Claims 12-15, 17 and 18 depend from claim 11 and are considered patentable for at least the same reasons.

Claim 21 recites "wherein the first message modification key value is determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient." As noted above, the combination of Labaton in view of Odagawa fails to teach this feature. Thus, claim 21 is patentable over Labaton in view of Odagawa.

I. Rejection of claims 8-10, 19 and 20

Claims 8-10, 19 and 20 were rejected under 35 U.S.C. § 103 as being unpatentable over Labaton in view of Odagawa and Kamperman. This rejection is traversed for the following reasons. Kamperman was relied upon for disclosing

transmitting modified data messages, but fails to cure the deficiencies of Labaton in view of Odagawa discussed above with reference to claims 1 and 11. Claims 8-10 depend from claim 1 and claims 19 and 20 depend from claim 11, and are patentable over Labaton in view of Odagawa and Kamperman for at least the reasons advanced with reference to claims 1 and 11.

III. Conclusion

In view of the foregoing, it is respectfully requested that the appealed rejections be reversed.

In the event the Commissioner of Patents and Trademarks deems additional fees to be due in connection with this application, Applicants' attorney hereby authorizes that such fee be charged to Deposit Account No. 06-1130.

Respectfully submitted,

By:_____

David A. Fox
Registration No. 38,807
CANTOR COLBURN LLP
20 Church Street
22nd Floor
Hartford, CT 06103-3207
Telephone (860) 286-2929
Facsimile (860) 286-0115
Customer No. 36192

Date: April 22, 2009

CLAIM APPENDIX

1. A method for transmitting data over a computer network to a predetermined recipient, the method comprising:

modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message, the first message modification key value being determined based on at least one variable parameter;

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message, the second message modification key value being determined based on at least one variable parameter;

transmitting the first and second modified data messages to a first device;

determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value; and

determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value,

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message;

wherein the first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient.

2. The method of claim 1 wherein the variable parameter comprises a time-varying parameter.

3. The method of claim 2 wherein the time-varying parameter includes at least one of a determined hour, minute, and second.

4. The method of claim 1 wherein the biometric identifier obtained from the recipient is a voice sample of the recipient.

6. The method of claim 1 further comprising transmitting the first and second message modification key values to a first computer.

7. The method of claim 1 wherein the first and second modified data messages are both transmitted via a first communication channel.

8. The method of claim 6 wherein the first and second message modification key values are both transmitted via a second communication channel.

9. The method of claim 1 wherein said first data message comprises voice data.

10. The method of claim 1 wherein said first data message comprises video data.

11. A system for transmitting data over a computer network to a predetermined recipient, the system comprising:

a first device configured to modify at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message, the first message modification key value being determined based on at least one variable parameter, the first device further configured to modify at least one data byte in a second data message based on a second modification key value to obtain a modified second data message, the second message modification key value being determined based on at least one variable parameter, the first device configured to transmit the first and second modified data messages; and

a second device configured to receive the transmitted first and second modified data messages and to determine the first data message for the predetermined recipient based on the modified first data message and the first message modification key value, the second device further configured to determine the second data message for the

predetermined recipient based on the modified second data message and the second message modification key value,

wherein the first device is configured to modify multiple bytes of a first data message by adding the first message modification key byte value to multiple bytes of the first data message;

wherein the first message modification key value is determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient.

12. The system of claim 11 wherein the first and second devices comprise first and second computers, respectively, operatively communicating with one another.

13. The system of claim 11 wherein the variable parameter comprises a time-varying parameter.

14. The system of claim 13 wherein the time-varying parameter includes at least one of a determined hour, minute, and second.

15. The system of claim 11 wherein the biometric identifier obtained from the recipient is a voice sample of the recipient.

17. The system of claim 11 wherein the first device is further configured to transmit the first and second message modification key values to the second device.

18. The system of claim 11 wherein the first and second modified data messages are transmitted via a first communication channel.

19. The system of claim 11 wherein said first data message comprises voice data.

20. The system of claim 11 wherein said first data message comprises video data.

21. A computer-readable storage medium encoded with computer-readable computer program code for transmitting data over a computer network, the storage medium including instructions for causing at least one network element to implement a method comprising:

modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message, the first message modification key value being determined based on at least one variable parameter;

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message, the second message modification key value being determined based on at least one variable parameter;

transmitting the first and second modified data messages to a first device;

determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value; and

determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value,

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message;

wherein the first message modification key value is determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient.

EVIDENCE APPENDIX

Not Applicable

RELATED PROCEEDINGS APPENDIX

Not Applicable